

REMARKS

Claims 1-5, 7-9, 11-13, 15 and 16 are pending in this application. Initially, applicants extend their appreciation to Examiner Moorthy for the indication of the allowability of claims 1-5, 7-9, 11-13 and 15-17 at paragraph 7 of the November 24, 2006, Office Action.

In the outstanding Office Action, the Examiner rejected all of these pending claims under 35 U.S.C. § 112, second paragraph, as indefinite. The Examiner asserts at paragraph 5 of the Office Action that the claims are indefinite because the independent claims set forth that the coin has been signed in a step that precedes the step of encryption, but that the claim language renders the claim indefinite because it is not clear to the Examiner how there can be an encrypted copy of the unsigned coin after the coin has already been signed. At paragraph 6 of the Office Action, the Examiner further rejects claims 1-5, 7-9, 11-13 and 15-17 under 35 USC § 112, second paragraph, as being incomplete for omitting an essential step: forming a copy of an unsigned coin or unit being fully anticipated by U.S. Patent 6,237,095 to Curry, et al. (Curry).

Applicants respectfully disagree that the claims are indefinite or incomplete as asserted at paragraphs 5 and 6 of the Office Action.

As explained in detail in the present application, the instant invention provides a procedure to create and to use electronic cash. With a preferred embodiment of the invention, a customer sends to a bank a request for digital cash and a public key of an encryption scheme of the customer. The bank signs the cash using a secret key of the bank's own digital signature scheme, and encrypts the signature by using the public key provided by the customer. The bank

also encrypts, using the public key given to the bank by the customer, an unsigned copy of the cash. A copy of the encrypted signed cash and a copy of the encrypted unsigned cash are both sent to the customer by the bank.

In this case, the cash is the coin.

The customer then decrypts both of these copies – that is, both the signed and unsigned coin (copies of the cash) by using the private key of the customer’s encryption scheme. The customer then uses this decrypted, signed and unsigned pair of copies (coins) for payment to a third party. The third party, using these decrypted signed and unsigned copies of the cash (coins), can then ask the bank to confirm the validity of the digital cash. If that validity is confirmed, this third party is able to redeem the digital cash (coin) for payment.

An important feature of the present invention is that the bank encrypts both the signed and unsigned copies of the digital cash (coin) using the public key of the customer’s encryption scheme – that is, the customer has the private key of that encryption scheme. Then, both encrypted copies – that is, the encrypted copy of the signed coin and the encrypted copy of the unsigned coin - are sent back to the customer. Because of this feature, the customer, and only the customer, is able to decrypt both the signed and unsigned copies of the digital cash by using the private key of the customer’s encryption scheme. In this way, only the customer is able to control the use of these copies.

With respect to the Section 112, second paragraph rejection at paragraph 5 of the Office Action, applicants respectfully assert that the invention includes that there is encryption of both an unsigned copy of the coin and a signed copy of the coin. As mentioned, the specification and independent claim language clearly recite that the unsigned coin is sent to the coprocessor, where it is signed, and wherein the coprocessor encrypts both the signed coin and an unsigned copy of the coin (that is, the coin as it was sent to the coprocessor). Applicants respectfully assert that the skilled artisan will readily understand that a coin received may be processed by signing, or processed by encrypting, or processed by first signing the received coin and subsequently encrypting. Applicants further assert that where making a copy of a coin, or encrypted coin, etc. is within common knowledge of the skilled artisan where a copy is required to accomplish a cryptographic task.

Applicants believe that the specification makes clear that there is indeed an encrypted copy of an unsigned coin as well as an encrypted copy of the coin as signed, and that receiving and signing a coin, and encrypting the signed coin does not exclude that a copy of the received unsigned coin may be encrypted after a copy is signed and encrypted. Accordingly, the withdrawal of the rejection of claims 1-5, 7-9, 11-13 and 15-17 under 35 USC § 112, second paragraph as indefinite is respectfully requested.

With respect to the rejection at paragraph 6 of the Office Action, applicants respectfully assert that the fact that the independent claims do not expressly recite, “forming a copy of an unsigned coin or unit” does not render those claims incomplete for omitting essential steps. As mentioned above, the specification and independent claim language clearly recites:

“the user sending a coin to be digitally signed to the coprocessor using any secure digital signature algorithm.”

A “coin,” as used in the independent claims, should be readily understood to the skilled artisan by a careful reading of applicants’ specification, drawings and claims as filed. That is, and as set forth in the independent claims, a coin may be generated in any way known to the skilled artisan, without limiting the scope or spirit of the invention in any way. Put another way, while the use of the coin as set forth in the independent claim language is essential to the invention, the manner in which a coin is formed or chosen or generated or defined is not essential to the invention as described, nor is it necessary to practice the steps as claimed. MPEP 2172.01.

For example, at page 10 of applicants’ specification, it is set forth that :

When ordering cash, customer C communicates to the secure cryptography generator SCG at the bank B (preferably using some secure channel on which both SCG and B can read), its own public encryption scheme (method belonging to List1, and key, all together denoted as Encr2), and orders some cash amount, with a description of the way to cut the amount into units, in a way compatible with List2 (for instance List2 will comprise all amounts available with regular coins and bills in the currency of interest to the customer). Each unit, Unit, is signed by the secure cryptography generator, and the signature Sign1(Unit) is then encrypted as Encr2(Sign1(Unit)) by SCG using the customer’s public encryption scheme.

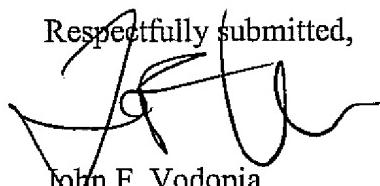
The SCG also computes Encr2(Unit). Besides the value, Val(Unit), of the unit, and preferably an expiration date, Exp(Unit), Unit comprises a large random number generated by SCG, in such a way that the same number will never reappear in further transactions, and possibly a secret version of that number provided by SCG, using a very secure method such as a one time pad. The SCG then communicates the quadruple

The coin may be the “orders” of some “cash amount,” as stated, or a “description” of an “amount” cut into units, as set forth. The coin may comprise the value (Val(unit)), or the unit,

and the unit may comprise a large random number generated ... More, in discussing basic cryptography, the application at page 2, line 11, refers to coins as known in the art of cryptography. "The basic idea is as follows. Customer C will choose a message x which is going to be the coin." Hence, a limitation of "forming a copy of an unsigned coin or unit" is not required for claims 1-5, 7-9, 11-13 and 15-17 to comply with the second paragraph of 35 USC § 112, and applicants respectfully request withdrawal of the rejection of the claims.

For the reasons discussed above, the Examiner is asked to reconsider and to withdraw the final rejections of claims 1-5, 7-9, 11-13 and 15-17 under 35 U.S.C. 112, second paragraph, and to allow the claims. If the Examiner believes that a telephone conference with Applicants' Attorneys would be advantageous to the disposition of this case, the Examiner is requested to telephone the undersigned.

Respectfully submitted,



John F. Vodopia
Registration No. 36,299
Attorney for Applicants

Scully, Scott, Murphy & Presser, P.C.
400 Garden City Plaza, Suite 300
Garden City, New York 11530
(516) 742-4343

JFV:gc